TRADING PARTNER AGREEMENT

This Trading Partner Agreement (hereinafter "Agreement"), effective 1 November 2005, is made by and between the Commonwealth of Kentucky Cabinet for Health and Family Services ("CHFS"), Department of Medicaid Services ("DMS"), and _____, a _____ corporation with its principal place of business at _____, _____, _____, _____ ("Provider"), a licensed health care provider.

WHEREAS, Provider renders certain professional health care services ("Services") to members of employer groups and individuals, and submits documentation of those Services to DMS; and,

WHEREAS, DMS, in its implementation of the Medicaid program in Kentucky, provides to health care companies such as Provider a System of operational and informational support to respond to member and provider inquiries to exchange certain claims and billing information through electronic communications and through the Internet (hereinafter the "System");

WHEREAS, while performing its services Provider may be given access to, or may be exposed to, certain confidential or Individually Identifiable Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 Code of Federal Regulations Parts 160-164, and applicable regulations that implement Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq*. (the "GLB Regulations");

WHEREAS, Provider desires to utilize the System provided by DMS, and DMS desires to provide the System and related services and support to Provider, as defined and according to the terms contained hereinafter.

WHEREAS, as a condition of Provider's engagement by DMS, Provider agrees to take certain precautions, comply with certain practices, and implement certain procedures required by applicable law for the purposes of guarding data integrity and safeguarding the confidentiality of Protected Health Information, all as more specifically set forth in this Agreement; and

NOW, THEREFORE, in consideration of the premises and the mutual covenants and agreements hereinafter set forth, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Provider and DMS (collectively, the "Parties") agree as follows:

1. **DEFINITIONS.**

   a. **"Companion Guides."** aka "Guide" here within the TPA. Companion Guide will be created to help assist submitters in their submission of claims to DMS.

   b. **"Data."** Any information provided and/or made available by either of the Parties to the other, and includes, but is not limited to enrollment and eligibility data, claims data, and PHI.

   c. **"Electronic Data Interchange ("EDI") Companion Guide."** A technical user's manual provided to Provider to assist Provider in preparing and completing electronic data

interchange. DMS reserves the right to revise and update the EDI Companion Guide ("Guide") in its sole discretion.

d. **"Electronically Maintained."** Information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

e. **"Electronically Transmitted."** Information exchanged with a computer or electronic device using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, and private networks, but excluding information exchanged using paper-to-paper facsimiles, person-to-person telephone calls, video teleconferencing, voice mail messages, telephone voice response or "fax-back" systems.

f. **"Health and Human Services ("HHS") Privacy Standard Regulation."** 45 Code of Federal Regulations ("C.F.R.") at Title 45, Parts 160 through 164.

g. **"Health and Human Services ("HHS") Security Standard Regulation."** 45 Code of Federal Regulations ("C.F.R.") at Title 45, Parts 160, 162 and 164.

h. **"HHS Standard Transaction Regulation."** 45 C.F.R. Parts 160 and 162.

i. **"Individual."** The person who is the subject of the Data, as defined by 45 C.F.R. §164.501.

j. **"Individually Identifiable Health Information."** Health information, including demographic information collected from an individual, and that (i) is created by or received from DMS; and (ii) relates to the past, present, or future physical or mental health or condition of an individual, the provisions of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

k. **"Privacy Regulations."** The Standards for Privacy of Individually Identifiable Health Information (64 Fed. Reg. 59918 (1999)) and any and all amended or additional proposed regulations and final rules generated pursuant thereto.

l. **"Proprietary Data."** Information used or created by DMS in the conduct of its activities that is not normally made available to parties outside of DMS, the disclosure of which will or may be detrimental to DMS' ongoing activities that Provider would not otherwise have access to but for its relationship with DMS.

m. **"Protected Health Information."** Individually Identifiable Health Information that is or has been Electronically Transmitted or Electronically Maintained by DMS and communicated to Provider and includes such information in any other form (e.g., paper printouts, tapes, notes).

n. **"Regulations."** Collectively, the Privacy Regulations and the Security Regulations.

o. **"Security Regulations."** The Security and Electronic Signature Standards (63 Fed. Reg. 43242 (1998)) and any and all amended or additional proposed regulations and final rules generated pursuant thereto.

2. **INTRODUCTION.** This Agreement authorizes the Parties to electronically exchange Data, including PHI, through a public or private telecommunications network using language and code sets authorized at 45 C.F.R. § 160 et seq., in an efficient and cost-effective manner without limiting the obligations of each party as set forth in this Agreement or imposed by applicable law, solely for the purposes set forth herein, in accordance with the terms "Standard" and "Transactions" as defined at 45 C.F.R. § 160.103 (hereinafter aggregated and referred to as "Standard Transactions"), the privacy standards described and referenced below, and requirements for non-standard transactions (if applicable).

Any Data, Proprietary Data or PHI exchanged under this Agreement is to be used and exchanged solely as authorized by HIPAA, and is further subject to the terms and conditions set forth in this Agreement. Provider acknowledges that coverage for any services furnished by Provider and electronically exchanged through this Agreement is subject to the terms and conditions of the individual's benefit program, any agreement between Provider and DMS, and DMS' regulations, policies, and procedures.

3. **DMS OBLIGATIONS.**

a. **ID(s) and Password(s).** Upon execution of this Agreement, DMS will assign logon ID(s) and password(s) to Provider to allow Provider to authenticate its identity and transmit data electronically. DMS shall retain title to all logon ID(s) and password(s), and reserves the right to change any logon ID or password at any time, for any reason, or if required to do so by law, regulation, or court order.

b. **System.** DMS shall design and implement an interface between DMS's and Provider's computer systems, but all computer programming on Provider's side of the interface shall be the responsibility of Provider. DMS shall provide to all Users of the System a toll-free number and an e-mail address to assist with questions or problems.

c. **Data.** The Data the Parties may exchange pursuant to this Agreement may change as a result of changes in law or regulation, or actions taken by an employer group in accordance with the terms and conditions of certain health care benefits contracts, or changes made to those contracts. DMS' response to inquiries does not guarantee coverage. Acceptance by DMS of the Data Provider sends electronically does not constitute guarantee of reimbursement.

4. **PROVIDER OBLIGATIONS and AUTHORIZATIONS.**

a. **Provision of Data.** Provider may provide DMS Data electronically, including the

minimum necessary PHI (see 45 C.F.R. § 164.502(b)) in accordance with the terms of the Agreement and the Guide. Provider is solely responsible to ensure that the Data it provides DMS is correct.

b. **Logon ID and Password.** Provider agrees to protect DMS' logon ID(s) and password(s) from compromise, release or discovery by any unauthorized person, and shall not disclose logon ID(s) and password(s) to any third party in any manner. A breach of this provision shall be considered material. In the event a breach occurs, Provider must notify DMS immediately. Provider acknowledges and agrees that only Provider personnel it designates shall be permitted to use the logon ID(s) and password and only within the scope of the approved application. Provider's use of logon ID(s) and password(s) constitutes an Electronic Signature that confirms Provider's willingness to remain bound by these terms and conditions and ratify any transaction conducted electronically by DMS. In the event of logon ID(s) and/or password(s) are compromised, Provider shall be responsible for such ramifications resulting from Provider's failure to protect DMS logon ID(s) and password(s).

c. **System Technical Issues.** Provider shall provide DMS with detailed information and documentation regarding the compatibility requirements of Provider's system, including data information such as required file structures and field descriptions. Provider shall designate individuals within its organization to serve as liaisons with DMS regarding technical matters, Plan Information communications and user-related questions;

d. **Provider's Costs.** Provider shall be solely responsible for all of its costs to transmit, access and receive Data electronically including, but not limited to, the costs of computers, terminals, connections, modems, software and browsers that have the capability to use HIPAA mandated code-set Standard Transactions, and the costs of providing sufficient security measures to safeguard receipt and transmission of PHI in accordance with 42 USC § 1320d-2(d), 45 C.F.R. § 164.530 and the implementing regulations issued by HHS or DMS to preserve the integrity and confidentiality of, and to prevent non-permitted use or violations of disclosure of PHI. Provider acknowledges that any changes made to Data may impact any reimbursement it receives.

e. **Authorization to Use Data.** Provider's use of a DMS system or process under this Agreement constitutes authorization and direction to DMS to use the PHI or other Data received from the Provider to adjudicate and process health care claims DMS receives from Provider. Provider acknowledges that DMS may disclose the PHI it makes available to DMS concerning Individuals who are members of a plan to the plan sponsor or the group health plan consistent with HIPAA's requirements and the language set forth herein.

f. **Testing.** Prior to the initial data transmission for each type of transaction, Provider will test and cooperate with DMS in testing Provider's operating system to ensure the accuracy, timeliness, completeness, compatibility, and confidentiality of each data transmission.

g. **Limited Access.** Provider will not obtain access by any means to data or DMS' operating system for any purpose. In the event Provider receives data not intended for Provider, Provider will immediately notify DMS and delete the data from its operating system.

h. **Notice of License Impairment.** Provider shall notify DMS immediately in writing of any existing or subsequent suspension or revocation of Provider's license or certificate, or exclusion of participation in the Medicare, Medicaid, or any other federal program.

5. COMPLIANCE WITH STANDARD TRANSACTIONS. When required, the Parties shall comply with each applicable regulation when performing "Standard Transactions." The Parties will not enter into any Trading Partner Agreement related to this Agreement that: changes any definition, data condition or use of a data element or segment, nor adds any data elements or segments to the maximum defined data set as proscribed in the HHS Transaction Standard Regulation, and as further proscribed by DMS. (See 45 C.F.R. § 162.915(b)). The Parties further agree that they will neither use any code or data elements marked "not used" or which are not found in the HHS Transaction Standard's implementation specifications, nor change the meaning or intent of any of the HHS Transaction Standard implementation specifications. (See 45 C.F.R. § 162.915(c) (d)).

Provider further agrees as follows:

a. **No Changes.** Provider hereby agrees that it will not change any definition, data condition or use of a data element or segment as proscribed in the HHS Transaction Standard Regulation. (ref. 162.915(a));

b. **No Addition**s. Provider hereby agrees that it will not to add any data elements or segments to the maximum denied data set as proscribed in the HHS Transaction Standard Regulation. (ref. 162.915(b));

c. **No Unauthorized Uses.** Provider hereby agrees that it will not to use any code or data elements that are either marked "not used" in the HHS Transaction Standard's implementation specifications or are not in the HHS Transaction Standard's implementation specifications. (ref. 162.915(c));

d. **No Changes to Meaning or Intent.** Provider hereby agrees that it will not to change the meaning or intent of any of the HHS Transaction Standard's implementation specifications. (ref. 162.915(d));

e. **Concurrence for Test Modifications to HHS Transaction Standards.** Provider agrees and understands that there exists the possibility that Provider or others may request an exception from the uses of a standard in the HHS Transaction Standards. If this occurs, Provider agrees that it will participate in such test modification. (ref. 162.904(a)(4));

f. **Incorporation of Modifications to HHS Transaction Standards.** Provider agrees and understands that from time-to-time, HHS may modify and set compliance dates for the

HHS Transaction Standards. Provider agrees to incorporate by reference into this Agreement any such modifications or changes. (ref. 160.140);

g. **Code Set Retention (Only for Plans).** Both Parties understand and agree to keep open code sets being processed or used in this Agreement for at least the current billing period or any appeal period, which ever is longer. (ref. 162.925(c)(2)); and

h. **Property Rights.** The Information shall be and remain the property of DMS. Provider agrees that it acquires no title or rights to the Information, including any de-identified information, as a result of this Agreement.

6. COMMUNICATIONS DETAILS. This Communications Details section defines the protocol for establishing electronic data interchange (EDI) connectivity and the protocol for transaction transmissions:

a. **MAP Agreements.** EDI Trading Partners must execute pertinent MAP Agreements. The MAP 246 agreement is pertinent to EDI Trading Partners acting as a billing agent; the MAP 380 agreement is pertinent to EDI Trading Partners engaging in electronic data interchange with DMS.

b. **EDI Enrollment.** This section defines the protocol new EDI trading partners must follow to test and ultimately be permitted to transmit transactions into production adjudication systems.

Enrollment to become an EDI Trading Partner is a five-step process. The steps that must be completed are:

(1) Contact CHFS EDI Department;
(2) Acquire Current EDI Interface Documentation;
(3) Retain an EDI Interface Logon ID and Password;
(4) Complete EDI Testing; and
(5) Maintain Production Standards.

(1) Contact CHFS EDI Department. Prospective EDI Trading Partners must contact the CHFS EDI Technical Support Help Desk by phone as provided on the contact information sheet to be supplied by CHFS. CHFS will initiate the EDI enrollment process by acquiring trading partner demographic information such as organization name, contact person(s), phone number(s) and email addresses.

(2) Retain Current EDI Interface Documentation. CHFS Technical Support Representative will review the prospective EDI Trading Partner's EDI Interface documentation for accuracy, completeness, and currency to continue the EDI enrollment process. If the trading partner does not have accurate, complete, and current documentation, the EDI Technical Support Representative will make arrangements to disseminate the documentation. EDI Interface documentation will evolve as HIPAA and business needs arise. Trading Partners may contact the

CHFS EDI Technical Support Help Desk or use the various EDI interfaces themselves to acquire current documentation.

(3) EDI Interface Logon ID and Password. CHFS EDI Technical Support Help Desk is the only entity permitted to assign and maintain trading partner EDI interface logon ID and passwords. Every prospective EDI Trading Partner is assigned a single logon ID and password by the CHFS EDI Technical Support Help Desk.

(4) EDI Testing. There are two phases of EDI Trading Partner testing, both of which must be passed before an EDI Trading Partner may transmit transaction data into adjudication environments. CHFS EDI Technical Support Representatives will assist trading partners through both phases of testing. Trading Partners that have acquired a third party HIPAA certification are not exempt from either phase of testing.

(a) Communications Testing. EDI Trading Partners must demonstrate to DMS's satisfaction their ability to establish a reliable electronic communications connection with the EDI interface being tested (Internet or Dial-up).

(b) Transaction Testing. The EDI Trading Partner must independently transmit the transaction file to be tested into the EDI interface being tested. Test transaction data must be de-identified by the trading partner prior to it being sent to CHFS. Test transmission files must contain a minimum of thirty transactions to be considered for testing. The transactions within the test transmission must be pertinent to the type of billing normally performed by the testing partner. Only one transaction type per transmission file is permitted. This limits test and production data to a single ISA-IEA Interchange control structure. CHFS will require trading partners that bill for specific provider's types to test certain transaction scenarios. A list of these constraints is shown in the CHFS document *Provider Type EDI Testing Constraints*. This list will evolve as business needs arise. Trading partners will be notified if they need to test certain transaction scenarios when they contact the CHFS EDI Technical Support Help Desk to begin testing. CHFS will test the transactions for up to seven phases of HIPAA compliance as defined by X12. Once a trading partner has successfully tested, it will be permitted to transmit the transaction type and version tested into the EDI interface tested. Trading partners must satisfactorily test with each transaction type, transaction version and interface desired.

(5) Maintain Production Standards. EDI Trading Partners that have successfully completed the previous four steps of the EDI Trading Partner enrollment process will be able to exchange data in production environments. To protect the integrity of the EDI interfaces, CHFS may revoke any EDI Trading Partner's access to the System at any time.

c. **Standard EDI Interfaces.** This section details various standard electronic data interchange interfaces that CHFS supports.

Kentucky Medicaid offers four standard EDI interfaces:

(1) Internet Direct Data Entry;
(2) Internet Batch File Upload and Download;

(3) Dial-up System; and
(4) CD/Diskette.

These interfaces are defined below. Trading partners unable to submit transactions on any of these standard EDI interfaces should contact the CHFS EDI Technical Support Help Desk for assistance on a case-by-case basis. Constraints that apply to <u>all</u> of the EDI interfaces are:

- Once an EDI Trading Partner is assigned an interface logon ID and password by the CHFS EDI Technical Support Help Desk, that logon ID and password may be used to access all EDI interfaces.

- A trading partner may utilize one or all of the interfaces available to them at any time.

- Trading partners may not exceed fifty EDI file transmissions per day per transaction type (constraints on physical media, such as CD/Diskette, are more stringent).

The following are specific constraints related to each EDI interface.

(1) Internet Direct Data Entry ("IDDE").

a) The IDDE EDI interface is replacing existing DMS proprietary non-HIPAA compliant freely distributed software. Non-HIPAA compliant transactions will not be accepted.

b) The IDDE interface resides within a secure area. Only approved EDI Trading Partners will have access to IDDE. If your organization requires access to IDDE, contact the CHFS EDI Technical Support Help Desk for assistance.

c) IDDE allows users to key Professional, Institutional, Dental and/or Pharmacy transactions directly into CHFS servers for adjudication. Additional functions and features may be added at the discretion of DMS to aide in business functions.

d) IDDE is a single-transaction system not a batch submission system. Transactions are keyed and submitted for adjudication one at a time rather than in batch format.

e) The client workstation system requirements for IDDE are that the workstation must have Internet connectivity and a modern web browser as defined by on the interface itself.

f) The IDDE EDI interface is generally available without interruption. Every attempt will be made to minimize maintenance unavailability.

g) Transactions accepted prior to Friday at 3:00 p.m. Eastern Standard Time will generally process in the current adjudication cycle. Transactions accepted after Friday at 3:00 p.m. Eastern Standard Time may not be processed until the following adjudication cycle.

h) Periodic revisions will be made to the IDDE interface to maintain HIPAA compliance and trading partner usability.

i) Current, detailed configuration and instructions regarding the IDDE EDI interface are available in the 'Internet Direct Data Entry Interface User Manual'. This manual is maintained by the CHFS EDI Technical Support Help Desk.

(2) Internet Batch File Upload and Download ("IBFUD").

a) This interface resides within a secure area. Only approved EDI Trading Partners will have access to IBFUD functions. If your organization requires access to IBFUD functions, contact the CHFS EDI Technical Support Help Desk for assistance.

b) IBFUD allows trading partners to submit and retrieve X12 HIPAA compliant transaction files adopted by DMS. Additional functions and features may be added at the discretion of DMS to aide in business functions.

c) IBFUD is a batch submission system EDI interface. EDI Trading Partners are solely responsible for acquiring and maintaining third party application software to generate and/or retrieve and translate X12 HIPAA compliant batch transaction files.

d) The client workstation system requirements for the Internet Batch File Upload and Download electronic data interchange interface are that the workstation must have Internet connectivity and a modern web browser.

e) The Internet Batch File Upload and Download electronic data interchange interface is available twenty-four hours a day, seven days a week, three hundred sixty-five days a year. Every attempt will be made to minimize maintenance unavailability.

f) Transmissions accepted prior to Friday, 3:00pm eastern-standard time will process in the current adjudication cycle. Transmissions accepted after Friday, 3:00pm eastern-standard time may not be processed until the following adjudication cycle.

g) Periodic revisions will be made to the Internet Batch File Upload and Download electronic data interchange interface to maintain HIPAA compliance and trading partner usability.

h) Current, detailed configuration and instructions regarding the Internet Batch File Upload and Download electronic data interchange interface are available in the 'Internet Batch File Upload and Download Interface User Manual'. This manual

is maintained by the CHFS Electronic Data Interchange Technical Support Help Desk.

(3) Dial-up System ("DUS").

a) The DUS interface resides within a secure area. Only approved EDI Trading Partners will have access to the DUS interface. If your organization requires access to the DUS interface, contact the CHFS EDI Technical Support Help Desk for assistance.

b) The DUS interface allows approved EDI Trading Partners to submit and retrieve X12 HIPAA compliant transaction files adopted by DMS. Additional functions and features may be added at the discretion of DMS to aide in business functions.

c) The DUS is a batch submission system EDI interface. EDI Trading Partners are solely responsible for acquiring and maintaining third party application software to generate and or retrieve and translate X12 HIPAA compliant batch transaction files.

d) The client workstation system requirements for the DUS are that the workstation must have asynchronous communications software and a modem capable of at least 28.8bps.

e) The Dial-up System interface is available twenty-four hours a day, seven days a week, three hundred sixty-five days a year. Every attempt will be made to minimize maintenance unavailability.

f) Transmissions accepted prior to Friday, 3:00pm eastern-standard time will process in the current adjudication cycle. Transmissions accepted after Friday, 3:00pm eastern-standard time may not be processed until the following adjudication cycle.

g) Periodic revisions will be made to the Dial-up System electronic data interchange interface to maintain HIPAA compliance and trading partner usability.

h) Current, detailed configuration and instructions regarding the Dial-up System electronic data interchange interface are available in the 'Dial-up System User Manual'. This manual is maintained by the CHFS Electronic Data Interchange Technical Support Help Desk.

(4) CD / Diskette.

a) CHFS will accept CD (standard 650MB formatting) and 3.5" IBM 1.44MB formatted diskette media in special circumstances where none of the other EDI are functioning. CD (standard 650MB formatting) and 3.5" IBM 1.44MB

formatted diskette submission of transmission files is considered a temporary medium until one of the other interfaces may be utilized.

b) Only approved EDI Trading Partners may submit transmissions via CD (standard 650MB formatting) or 3.5" IBM 1.44MB formatted diskette.

c) The physical media used in this interchange become the property of CHFS. Media may be destroyed. Media will not be returned.

d) A maximum of five physical media electronic data interchanges per week is allowed.

e) If the use of physical media is required beyond a three-month period a technical inquiry will be initiated to investigate alternatives.

d. Inbound Transactions. This section identifies HIPAA transactions that CHFS supports for billing and inquiry.

The CHFS document *HIPAA EDI Approved Transactions* identifies currently-approved inbound EDI transactions. Inbound transactions are used by Trading Partners to submit billing or inquiry transactions. The list of HIPAA EDI approved transactions will evolve as HIPAA, legislation and business needs arise. Trading Partners will be provided with a current copy of *HIPAA EDI Approved Transactions* upon request.

e. Outbound Transactions. This section identifies HIPAA transactions that CHFS supports for responding to trading partner inbound transactions.

The CHFS document *HIPAA EDI Approved Transactions* identifies currently-approved outbound EDI transactions. Outbound transactions are used by CHFS to respond to Trading Partner submitted billing or inquiry transactions. The list of HIPAA EDI approved transactions will evolve as HIPAA, legislation and business needs arise. Trading Partners will be provided with a current copy of *HIPAA EDI Approved Transactions* upon request.

f. Acknowledgement Transactions. This section identifies the acknowledgement transactions utilized by CHFS for electronic data interchange.

The CHFS document *HIPAA EDI Approved Transactions* identifies currently-approved acknowledgment EDI transactions. Acknowledgement transactions are used by CHFS to acknowledge receipt of Trading Partner submitted billing or inquiry transactions. The list of HIPAA EDI approved transactions will evolve as HIPAA, legislation and business needs arise. Trading Partners will be provided with a current copy of *HIPAA EDI Approved Transactions* upon request. CHFS will not accept negative control numbers in the ISA Control Number Element. Transmissions will be rejected if negative numbers are sent in the ISA Control Number Element. Negative Control Numbers will be treated as invalid. This error condition will be reported in the TA1 Interchange Acknowledgement.

7. COMPLIANCE WITH PRIVACY STANDARDS. Each party will develop, implement, maintain and use appropriate administrative, technical and physical Data safeguards, in compliance with 42 U.S.C. § 1320d-2(d), 45 C.F.R. § 164.530(c) and patient confidentiality provisions of applicable state statutes or regulations, and shall comply with any applicable GLB Regulations, or any amendments to any of these statutes or regulations.

Provider agrees to safeguard the Protected Health Information as follows:

  a. Provider agrees not to use or further disclose the Protected Health Information other than as permitted or required by this Agreement;

  b. Provider agrees to use appropriate safeguards to prevent any use or disclosure of the Protected Health Information that is not permitted or provided for by this Agreement;

  c. Provider agrees not to use or further disclose the Protected Health Information in a manner that, if undertaken by DMS, would violate the requirements of the Privacy Regulations;

  d. Provider agrees to provide a written report to DMS regarding any use or disclosure of the Protected Health Information not permitted or provided for by this Agreement of which Provider becomes aware within five (5) calendar days of Provider becoming aware;

  e. Provider agrees to provide DMS rights of access to any Protected Health Information that is in its possession, including rights to inspect and obtain copies of Protected Health Information for so long as the Protected Health Information is maintained;

  f. Provider agrees to incorporate any amendments or corrections to the Protected Health Information received from DMS when notified of such amendments or corrections by DMS;

  g. Provider shall make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from DMS available to the Secretary of the Department of Health and Human Services for the purposes of determining compliance with the Privacy Regulations; and

  h. Upon expiration or termination of this Agreement, at DMS's option, Provider shall either return or destroy all Protected Health Information received in any form from DMS within thirty (30) calendar days of the effective date of expiration or termination and shall not retain any copies of such Protected Health Information.

Each party shall execute Trading Partner, and/or Business Associate Agreements, acceptable to DMS, with subcontractors or agents that provide services involving maintenance, use or disclosure of PHI, ensuring that any subcontractors or agents to whom it provides PHI agree in writing to those restrictions that, with respect to such PHI, apply to that individual subcontractor or agent. Each party agrees that it will not maintain, use, make available or further disclose PHI other than as permitted or required by this Agreement or as required by law.

If any activity under this Agreement would cause any Provider to be considered a "Business Associate" of any other Party under 45 C.F.R. § 160.103, the following restrictions will apply to all uses and disclosures of PHI. The Business Associate will:

a. Not use or further disclose PHI other than as permitted or required by this Agreement, or to comply with judicial process or any applicable statute or regulation;

b. Notify the other Party in advance of any disclosure of PHI that the Business Associate is required to make under any judicial or regulatory directive;

c. Use appropriate safeguards to prevent use or disclosure of PHI other than for the purposes required in this Agreement;

d. Report to the other parties any use or disclosure of PHI not provided for in this Agreement of which the Business Associate becomes aware;

e. Ensure that any agents or subcontractors to whom the Business Associate discloses PHI received from another party, or created on behalf of another party, agrees to the same restrictions and conditions that apply to the protection of information under this Agreement;

f. Make PHI available to individuals as required by 45 C.F.R. § 164.524;

g. Make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526;

h. Make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528;

i. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or collected by the Business Associate on behalf of another Party, available to the Secretary of HHS when called upon for purposes of determining the other Party's compliance with federal privacy standards; and

j. At termination of this Agreement, if feasible, return or destroy all PHI received from another Party, or created or collected by the Business Associate on behalf of the other Party, that the Business Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, or if the PHI is still used to perform business functions, continue to treat all such PHI in accordance with the limits provided in this Agreement, and applicable law and regulation.

8. SYSTEMS AND PERSONNEL SECURITY: UNAUTHORIZED DISCLOSURES. The Parties shall comply with the final version of the data security standard promulgated by HHS (final version found at 45 C.F.R. Part 160, 162, and 164, published February 20, 2003, 68 Federal Register, Pages 8334-8381, the "Security Standard"). On or before the required

compliance date of the final Security Standard, the Parties will adopt any necessary modifications to their practices for maintaining PHI or transmitting PHI electronically, and shall provide any written assurances required under the final Security Standard to prevent unauthorized access to Data. If an unauthorized disclosure of PHI, or the discovery of unauthorized access to and/or tampering with the Data or DMS' Proprietary Data is discovered, the disclosing party will immediately report to the other party, using the most expeditious medium available, no later than five (5) calendar days after such discovery/disclosure is made, the following information:

    a. the nature of the disclosure;

    b. PHI used or disclosed;

    c. the individual(s) who made and received the disclosure;

    d. any corrective action taken to prevent further disclosure(s) and mitigate the effect of the current disclosure(s); and

    e. any such other information reasonably requested by the non-disclosing party.

The Parties will cooperate in the event of any litigation concerning unauthorized use, transfer or disclosure of such Data. Failure to adhere to this section may constitute violation(s) of applicable federal and state laws and regulations and may constitute just cause for immediate termination of this Agreement.

9. NOTICES. Any notice relating to this Agreement shall be in writing and transmitted by either (i) U.S. Mail, first class, postage prepaid; or (ii) facsimile transmission to the addresses/telephone numbers in this section below. Notices or communications shall be deemed given (a) in the case of transmittal by U.S. mail, on the date of receipt by the addressee; and (b) in the case of facsimile transmission, on the date the facsimile is sent.

Attn: _____   Attn: _____
Cabinet for Health and Family Services   Provider: _____
Department for Medicaid Services   Address: _____
275 East Main Street, Suite 6W-B   _____
Frankfort, KY 40621   _____
Fax: 502-564-   Fax: (_____) _____ - _____

10. RECORDS AND AUDIT. The Provider shall maintain, in accordance with their document retention policies and applicable law and regulation, but for a minimum of six (6) years, true and correct copies of any and all source documents from which they reproduce Data. DMS reserves the right to audit those records and security methods of Provider necessary to ensure compliance with this Agreement, to ensure that adequate security precautions have been made to prevent unauthorized disclosure or, to verify the accuracy and authenticity of the services underlying any EDI transaction.

11. TERM, TERMINATION and SUSPENSION. This Agreement shall become effective

upon execution, and shall remain in effect until terminated as provided below. Provider agrees that its ability to transmit, receive or otherwise electronically access Data will cease if Provider or DMS terminates this Agreement.

Either party may terminate this Agreement without cause upon sixty (60) days prior written notice.

Either party may terminate this Agreement immediately in the event of a material breach by the other party. A material breach shall include, but not be limited to, breach of any substantive term(s) of this Agreement, fraud, abuse, and/or failure to protect PHI. The terminating party may rescind notice of termination if the other party successfully cures the breach complained of to the terminating party's reasonable satisfaction. Each party may also temporarily suspend electronic communications under this Agreement to protect computer or data systems in cases of emergencies, or to perform maintenance. Each party agrees to minimize the frequency and duration of these temporary suspensions.

12. AUTOMATIC AMENDMENT FOR REGULATORY CHANGES. The parties recognize that this Agreement is subject to changes and amendments in the laws, regulations, and other lawful enactments or pronouncements and to the provision of any new legislation, regulations and case law affecting this Agreement. This Agreement will automatically amend to comply with any applicable statute, regulation, or amendment adopted by HHS or DMS, or applicable case law, concerning the subject matter of this Agreement upon the effective date of the statute, regulation, amendment, or court decision.

Any ambiguity in any term or condition of this Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA.

13. NO WARRANTY. DMS makes no warranty of any kind, express or implied, under this Agreement. Provider agrees that DMS shall not be responsible to Provider or anyone else for any damages caused by loss, delay, rejection, or any misadventure affecting such electronic information. DMS's sole liability to Provider or to any other person or entity in connection with DMS's responsibilities under this Agreement shall be to reprocess information supplied by Provider or duplicate information from a backup supplied by Provider upon DMS's request which shall be the sole remedy against DMS for claimed damage or injury of any nature. Provider specifically agrees that DMS shall not be liable for any consequential, indirect, special, incidental, exemplary or punitive damages under any circumstances, including, but not limited to, arising out of any access or use, or failure to access or use, or otherwise any reliance upon, the services DMS provides to Provider under this Agreement.

14. INDEMNIFICATION. Each party hereby recognizes and acknowledges that each party is responsible for its own conduct and the conduct of its officers, directors, employees and agents, and that each is responsible for any losses, liability, damages, costs and expenses that it incurs in the event that any claim is made by any person arising out of any of that party's acts or omissions related to this Agreement.

In the event that either party receives notice of any action, claim, or proceeding that alleges or

otherwise involves any act or omission of the other party, it shall promptly give notice to the other party and provide the other party with the opportunity and all reasonable assistance in the defense of such action. It is recognized that it may be necessary depending on the procedural status of the matter for one party to implead another party or to join it in litigation as a third party defendant.

In the event that the other party does not respond and defend, such other party shall indemnify the notifying party for any losses, liability, damages, costs and expenses that the notifying party incurs by reason of the failure of the other party to respond and defend; provided that it is understood that each party will carry errors and omissions insurance, and it is not intended that this Agreement should be interpreted or administered by the parties in any manner to invalidate any such insurance coverage.

Neither party shall be liable to the other party for damages caused by circumstances beyond its control, including, without limitation: "hackers" who gain access to the system or Data in spite of a party's commercially reasonable security measures, a major disaster, epidemic, the complete or partial destruction of its facilities, riot, civil insurrection, war or similar causes. Neither party shall be liable to the other party for any special, incidental, exemplary or consequential damages.

This section shall survive the termination of this Agreement.

15. SURVIVAL OF PROVISIONS. Any provision of this Agreement, which requires or reasonably contemplates the performance or existence of obligations by either party after the termination of the Agreement, shall survive such termination.

16. NO ASSIGNMENT. Neither this Agreement nor any right or interest herein may be assigned or transferred by either party in any manner, whether by operation of law or otherwise, without the prior written consent of the other party. Any purported assignment or transfer with the other party's consent shall be void. This Agreement shall otherwise be binding upon and shall inure to the benefit of the parties hereto, and each of their respective permitted successors and assigns.

17. NO MODIFICATION. This Agreement may not be altered, varied, revised or amended except in writing signed by both Parties. DMS reserves the right to amend the EDI Companion Guides, Application, and Forms from time to time.

18. NO WAIVER. No course of dealing or any failure of either party to enforce the rights, terms, provisions or remedies of this Agreement in a given instance shall be construed as a waiver thereof, and either such party shall retain the right to thereafter insist upon the other party's compliance therewith on any subsequent occasion.

19. FORCE MAJEURE. Neither party shall be deemed to be in default of this Agreement if prevented from performing any obligation hereunder for any reason beyond its control, including but not limited to, Acts of God, war, civil commotion, fire, flood or casualty. In any such case, the parties agree to negotiate in good faith with the goal of preserving this Agreement and the respective rights and obligations of the parties hereunder, to the extent reasonably practicable. It

is agreed that financial inability shall not be a matter beyond a party's control.

20. SEVERABILITY. If any portion of this Agreement shall, for any reason, be determined by a court of law to be invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable the entire Agreement, but rather the entire Agreement shall be construed as if not containing those invalid or unenforceable provision(s), and the rights and obligations of each party shall be construed and enforced accordingly.

21. RELATIONSHIP OF THE PARTIES. The parties to this Agreement intend that this Agreement will create a relationship of independent contractors between them. Nothing in this Agreement shall be construed as, or be deemed to create between the parties to this Agreement, a relationship of employer/employee or principal/agent or be construed to create a partnership, joint venture or agency relationship between DMS and Provider. Parties have no authority to represent each other as to any matters, except as expressly authorized in this Agreement.

22. CAPTIONS AND HEADINGS. The captions and headings throughout this Agreement are for convenience and reference only and are not intended to define, limit or describe the scope or intent of any provision of this Agreement.

23. GOVERNING LAW, JURISDICTION, AND VENUE. The laws of the Commonwealth of Kentucky shall govern the relationship of the parties and the construction, interpretation and performance of this Agreement and all transactions under it, except to the extent federal law preempts them. The state and federal courts in the Commonwealth of Kentucky shall have exclusive jurisdiction over any proceeding arising from or related to this Agreement, and any action, suit or proceeding arising from or related to this Agreement shall be brought in the appropriate state or Federal court in Franklin County, Kentucky.

24. ENTIRE AGREEMENT. This Agreement and any Manuals, Guides, Exhibits, Applications and Attachments thereto constitutes the entire Agreement between the Parties with respect to its subject matter. The provisions of this Agreement supersede all prior oral or written quotations, communications, agreements and understandings of the Parties with respect thereto.

SIGNATURES. The Parties will be bound by all the terms, provisions and conditions of this Agreement upon execution of the Agreement by each Party's authorized representative.

_____   _____
Company   Company

_____   _____
Signature   Signature

_____   _____
Name & Title   Name & Title